

Limiting Access to Inappropriate Internet Sites

Introduction

The Internet is probably the most important information resource of this century and yet it brings with it a host of challenges to management. Some key issues are the potential liability under sexual harassment and other laws, increased network vulnerability and lost productivity due to extensive non-business use of state owned information technology resources.

Purpose

The purpose of this policy is to define limitations of access to "inappropriate" Internet sites in concurrence with the "State of Utah Information Technology Resources Acceptable Use Policy," to address key management challenges associated with Internet use.

Statutory Authority

This policy is issued by the Chief Information Officer, pursuant to the Information Technology Act, Section 63D-1-301. This policy applies to all state agencies of the executive branch of government and its employees. It does not apply to employees or entities of the state's system of higher or public education.

Definitions

"State-provided information technology resource" means computer software, computer storage, electronic messaging and distribution systems, Intranet, the Internet, computer hardware and telecommunications equipment.

"Inappropriate Internet Site" means any site to which access would be inappropriate in the course of conduct of typical state business. Sites that fall under this definition include, but are not limited to: those that promote the use of alcohol, tobacco, gambling, illicit drug use and illegal activities; violence and violent extremist views including acts of extreme cruelty against animals or persons; full or partial nudity, and graphic sex.

Policy

It is the policy of the state of Utah to deploy and maintain a system designed to reasonably limit employees' access to inappropriate Internet sites while enabling state-provided information technology resource access for business purposes.

Individuals and groups of employees may request and receive an exemption from the department's or agency's senior executive or designee. An exemption request will identify the names of individuals or agency groups that are requesting the exemption and the stated business purpose for the exemption request. An exemption may be granted only when based upon an identifiable business need as determined by the department's or agency's senior executive or designee.

The State Information Security Committee, a subcommittee of the Information Technology Policy and Strategy Committee (ITPSC), will develop and periodically update, and the ITPSC will review and approve, a written operations plan for the deployment and maintenance of a system for limiting statewide access to inappropriate Internet sites by employees.

In deploying this technology the state understands the solution does not guarantee that all inappropriate sites that appear to fall within the definition can be fully and completely blocked. Nor does it contemplate that it can identify all sites that may be deemed inappropriate either now or in the future. Since access is limited based upon unique site identifying characteristics, it is reasonable to expect that sites wishing to prevent themselves from being blocked can frequently change their "identities" to avoid detection. For this reason cost-effective technology solutions require the frequent issuance of updates to keep products functioning as they were intended.